ON SOME APPLICATIONS OF PROBABILITY TO ANALYSIS AND NUMBER THEORY

P. ERDŐS

It would be quite impossible to give a survey of these subjects in a short article or lecture, and I will only succeed by making some arbitrary restrictions on the topics with which I will deal. First of all, I will restrict myself to problems and results on which I worked, and secondly, I will not discuss subjects which have been discussed in recently appeared review articles [**1**].

Probabilistic methods have been used in analysis for several decades; it suffices to name Paley, Wiener, Kolmogoroff, Zygmund, Salem, Steinhaus, Kac, Dvoretzky, Kahane, and many others. I will restrict myself to some questions my collaborators and I worked on for several years. Hardy was the first to give an example of a power series $\sum_{k=1}^{\infty} a_k z^{n_k}$ which converges uniformly in $|z| \leqslant 1$ but for which $\sum_{k=1}^{\infty} |a_k| = \infty$. Piranian asked me for what sequences of integers $n_1 < n_2 < \ldots$ does there exist a power series $\sum_{k=1}^{\infty} a_k z^{n_k}$ which converges uniformly in $|z| \leqslant 1$ but for which $\sum_{k=1}^{\infty} |a_k| = \infty$. I proved [**2**] by probabilistic methods that if the sequence $\{n_k\}$ satisfies

$$\liminf (n_j - n_i)^{1/(j-i)} = 1 \text{ where } j - i \to \infty \tag{1}$$

then such a power series exists. Zygmund [**3**] proved that if $n_{k+1}/n_k > c > 1$ then if $\sum_{k=1}^{\infty} a_k z^{n_k}$ converges for $|z| \leqslant 1$, $\sum_{k=1}^{\infty} |a_k| < \infty$. Thus (1) is certainly not far from being best possible, and it is quite likely that it is, in fact, best possible; in fact, Zygmund's theorem may remain true for every sequence which does not satisfy (1), in other words, for every sequence $\{n_k\}$ for which there exists an absolute constant c so that for every $i < j$

$$n_j - n_i > (1+c)^{j-i}. \tag{2}$$

Curiously enough, (1) occurred in a seemingly different context. Gaier and Meyer-König [**4**] call the radius defined by $z = re^{i\phi}$, $0 \leqslant \pi < 1$, singular for $f(z) = \sum_{n=1}^{\infty} a_k z^n$ if $f(z)$ is unbounded in every sector $|z| < 1$, $\phi - \epsilon < \arg z < \phi + \epsilon$ where $\epsilon > 0$. They showed that if $f(z) = \sum_{k=1}^{\infty} a_k z^{n_k}$ and $n_{k+1}/n_k > c > 1$, and if $f(z)$ is unbounded in $|z| \leqslant 1$, then every radius

Received 1 May, 1963.

[JOURNAL LONDON MATH. SOC., 39 (1964), 692–696]

is a singular radius. Rényi and I [5] showed by probabilistic methods that if $\{n_k\}$ satisfies (1) then there exists a power series $f(z)=\sum_{k=1}^{\infty} a_k z^{n_k}$ for which $a_k \geqslant 0$, $\sum_{k=1}^{\infty} a_k = \infty$, thus the positive real axis is a singular radius but no other radius is singular. In fact, $f(z)$ is bounded in $|z| \leqslant 1$ if a region $|z-1| < \epsilon$ is excluded (for every $\epsilon > 0$). It again seems quite possible that our theorem is best possible; in fact, perhaps if $\{n_k\}$ satisfies (2) then the theorem of Gaier and Meyer-König remains true, but we could prove nothing in this direction.

Finally using the methods of [5], Rényi and I solved the following problem of Zygmund [6]: A well-known theorem of Wiener [7] states that if $\sum_{k=1}^{\infty} (a_k \cos \lambda_k x + b_k \sin \lambda_k x)$ satisfies $\lambda_{k+1} - \lambda_k \to \infty$ and is the Fourier series of a function $f(x)$ in L_1, and if $f(x)$ is in L_2 in (α, β), $0 \leqslant \alpha < \beta \leqslant 2\pi$, then it is in L_2 in $(0, 2\pi)$. Zygmund now asked whether the same result remains true for L_p instead of L_2. We proved that for $p > 2$ the answer is negative. In fact, we showed that there exists for every $\epsilon > 0$ a function $f(x)$ in L_2 $(0 \leqslant x \leqslant 2\pi)$ with the Fourier series

$$\sum_{k=1}^{\infty} (a_k \cos \lambda_k x + b_k \sin \lambda_k x), \quad \lambda_{k+1} - \lambda_k \to \infty$$

which is bounded for $\epsilon < x < 2\pi - \epsilon$ but which does not belong to any $L_{2+\eta}$ for $\eta > 0$ in $(0, 2\pi)$. For $p < 2$ we could not make any contribution to the problem of Zygmund.

Let $\sum_{k=1}^{\infty} |a_k|^2 = \infty$. Put

$$f_t(z) = \sum_{k=1}^{\infty} \epsilon_k a_k z^k, \quad \epsilon_k = \pm 1, \quad t = \sum_{k=1}^{\infty} \frac{1+\epsilon_k}{2^{k+1}}.$$

It is well known that for almost all t, $\sum_{k=1}^{\infty} \epsilon_k a_k z^k$ diverges almost everywhere on the unit circle. Dvoretzky and I proved [8] that if c_k is a monotone sequence of positive numbers tending to zero and satisfying

$$\limsup_{k=\infty} \frac{\sum_{j=1}^{k} c_j^2}{\log (1/c_k)} > 0 \tag{3}$$

and if $|a_k| \geqslant c_k$ then for almost all t $\sum_{k=1}^{\infty} \epsilon_k a_k z^k$ diverges everywhere on $|z| = 1$. In particular, our theorem holds if $a_k > c/k^{\frac{1}{2}}$ $(c > 0)$. Further, we showed that there is a sequence a_k satisfying $|a_{k+1}| < |a_k|$ and $\sum_{k=1}^{\infty} |a_k|^2 = \infty$ so that for almost all t the series $\sum_{k=1}^{\infty} \epsilon_k a_k z^k$ has on every arc

of $|z|=1$ points of convergence whose power is that of the continuum. We could not decide whether (3) is best possible; in other words, is it true that if (3) is false then there exists a sequence $\{a_k\}$ for which $|a_k| \geqslant c_k$ and for which $\sum_{k=1}^{\infty} \epsilon_k a_k z^k$ has at least one point of convergence for almost all t?

I would just like to call attention to a problem in the probabilistic theory of polynomials and power series which I tried several times to solve, unfortunately without any success. Put

$$f_t(z)=\sum_{k=1}^{\infty} \epsilon_k z^k, \quad f_{t,n}(z)=\sum_{k=1}^{n} \epsilon_k z^k, \quad \epsilon_k=\pm 1, \quad t=\sum_{k=1}^{\infty} \frac{1+\epsilon_k}{2^{k+1}}.$$

Is it true that for almost all t

$$\lim_{n=\infty} \max_{|z|=1} |f_{t,n}(z)|/(n \log n)^{\frac{1}{2}} = C, \tag{4}$$

where C is independent of t? The proof of (3) seems very difficult. Salem and Zygmund [9] proved the following slightly weaker result: There exist two constants c_1 and c_2 so that for almost all t and sufficiently large $n > n_0(t)$

$$c_1(n \log n)^{\frac{1}{2}} < \max_{|z|=1} |f_{t,n}(z)| < c_2(n \log n)^{\frac{1}{2}}. \tag{5}$$

In (5) the proof of the upper bound is simple; the real difficulty is the proof of the lower bound.

A well-known theorem states the following [10]:

Let $n_1 < n_2 < \ldots$, $n_{k+1}/n_k > c > 1$, be an infinite sequence of real numbers and $\sum_{k=1}^{\infty} (a_k^2+b_k^2)$ a divergent series of real numbers satisfying

$$\lim_{N=\infty} (a_N^2+b_N^2)^{\frac{1}{2}} \left(\sum_{k=1}^{N} (a_k^2+b_k^2) \right)^{-\frac{1}{2}} = 0.$$

Then

$$\lim_{N=\infty} E_x \left| \left\{ \sum_{k=1}^{N} (a_k \cos 2\pi n_k x + b_k \sin 2\pi n_k x) \right.\right.$$

$$\left.\left. < w\left(\tfrac{1}{2} \sum_{k=1}^{N} (a_k^2+b_k^2)^{\frac{1}{2}} \right) \right\} \right| = \frac{1}{\sqrt{(2\pi)}} \int_{-\infty}^{w} e^{-u^2/2} du. \tag{6}$$

Recently I weakened the lacunarity condition in the case $a_k = b_k = 1$. In fact I proved [11] (using the method of moments) that if $n_1 < n_2 < \ldots$ is an infinite sequence of integers satisfying

$$n_{k+1} > n_k \left(1 + \frac{c_k}{k^{\frac{1}{2}}} \right) \tag{7}$$

where $c_k \to \infty$, then (6) holds if we assume $a_k = b_k = 1$. It is not hard to see that the theorem is no longer true for all sequences $\{n_k\}$ if $c_k \to \infty$ is

no longer assumed, but for special sequences, say $n_k = [c^{k^\alpha}]$, $\alpha > 0$, the theorem probably remains true, but probably could only be proved by deep number theoretical methods. (For $\alpha > \frac{1}{2}$ this follows from our theorem (*i.e.* (7) is satisfied), but I cannot prove it for $\alpha = \frac{1}{2}$.

I would like to mention, finally, some number theoretic results which I have recently obtained by probabilistic methods and which are not yet published.

1. To every ϵ_1 and ϵ_2 there exists an n_0 so that if $n > n_0$ and $m < 2^{(1-\epsilon_1)\log\log n}$, then all but $\epsilon_2 n$ integers $1 \leqslant u \leqslant m$ have divisors in every residue class mod m. The result is best possible in the following sense: If $m > 2^{(1+\epsilon_1)\log\log n}$ then the number of integers $u < n$ which have a divisor in any given residue class mod m is less than $\epsilon_2 n$ if $n > n_0(\epsilon_1, \epsilon_2)$. The proof of the second statement is comparatively simple and does not require probabilistic arguments.

The proof of the first statement depends on the following result, which seems to have independent interest: Let G_n be an abelian group having n elements, let $k = \left[\frac{(1+\epsilon)\log n}{\log 2}\right]$ and choose k elements $a_1, \ldots, a_k$ at random. Then for all but $o\left(\binom{n}{k}\right)$ choices of $a_1, \ldots, a_k$ every element of G_n can be represented in the form $\prod_{i=1}^{k} a_i^{\epsilon_i}$ where $\epsilon_i = 0$ or 1.

I was led to these questions by the following result of Sivasankaranarayanu Pillai: Denote by $Q^{(n)}$ the number of integers $m \leqslant n$ which do not have a divisor of the form $p(kp+1)$. Then

$$Q(n) < cn/\log\log\log n.$$

Using the above results, I proved

$$Q(n) = \left(1+o(1)\right)\frac{e^{-\gamma} n}{\log 2 . \log\log n}.$$

Let $a_1 < a_2 < \ldots$ be an infinite sequence of integers and denote by $f(n)$ the number of solutions of $n = a_i + a_j$. Sidon asked the following question (in connection with his work on lacunary trigonometric series): How slowly can the sequence $\{a_k\}$ grow so that $f(n)$ should be bounded? Rényi and I [**12**] proved by probabilistic methods that for every ϵ there exists a sequence $a_k < k^{2+\epsilon}$, $k = 1, 2, \ldots$ for which $f(n) < c_\epsilon$. We could not give an explicit construction of such a sequence and we could not decide if $a_k < k^{2+\epsilon}$ can be improved. An old and probably very difficult conjecture of Turán and myself states that if $a_k < ck^2$ then $\limsup_{n=\infty} f(n) = \infty$. We can only prove that the sums $a_i + a_j$ cannot be all different.

2. I proved several years ago [**13**] that the density of integers n which have two divisors d_1 and d_2 satisfying $d_1 < d_2 < 2d_1$ exists, but I could not

prove that it is 1. Unless I made a mistake I proved this recently; in fact, I showed that for every $\eta > 0$ the density of integers n which have two divisors d_1 and d_2 satisfying

$$d_1 < d_2 < d_1\left(1+\left(\frac{e}{3}\right)^{(1-\eta)\log\log n}\right) \tag{8}$$

is 1, but the density of integers n which have two divisors d_1 and d_2 for which

$$d_1 < d_2 < d_1\left(1+\left(\frac{e}{3}\right)^{(1+\eta)\log\log n}\right) \tag{9}$$

is 0. The proof of (8) is comparatively simple and does not require probabilistic methods.

References

1. Recently several review articles appeared on applications of probability to number theory, *e.g.*, M. Kac, "Probability methods in some problems of analysis and number theory", *Bull. American Math. Soc.*, 55 (1949), 641–665; see also: Kubilijus, *Uspehi Matem. Nauk.*, 11 (1956), 31–66; P. Erdős, *Proc. Internat. Congress of Math., Amsterdam* (1959) Vol. 3, 13–19.
2. P. Erdős, "On the uniform but not absolute convergence of power series with gaps", *Ann. Soc. Pol. Math.*, 25 (1952), 162–168.
3. A. Zygmund, *Studia Math.*, 3 (1931), 77–91.
4. D. Gaier und W. Meyer-König, "Singuläre Radien bei Potenzreihen", *Jahresbericht d.Dm.V.*, 59 (1956), 36–48.
5. P. Erdős and A. Rényi, "On singular radii of power series", *Publ. Math. Inst. Hung. Acad.*, 3 (1959), 159–169.
6. ———, "On a problem of Zygmund", *Stanford Studies in Math.*, and Stat. IV. (Essays in Honor of G. Pólya) (1962), 110–116; see also for a slightly weaker result P. Turán, "On a certain problem in the theory of power series with gaps", *ibid*, 404–409.
7. N. Wiener, "A class of gap theorems", *Annali di Pisa*, 3 (1934), 367–372.
8. A. Dvoretzky and P. Erdős, "Divergence of random power series", *Michigan Math. J.*, 6 (1959), 343–347; see also A. Dvoretzky, "On the covering of the circle by randomly placed arcs, *Proc. Nat. Acad. Sci. U.S.A.*, 42 (1956), 199–203.
9. R. Salem and A. Zygmund, "Some properties of trigonometric series whose terms have random signs", *Acta Math.*, 91 (1959), 245–301.
10. ———, "On lacunary trigonometric series (I) and (II)", *Proc. Nat. Acad. Sci. U.S.A.*, 33 (1947), 333–338 and 34 (1948), 59–62. For the history of this problem see the paper of Kac quoted in [1].
11. P. Erdős, "On trigonometric sums with gaps", *Publ. Math. Inst. Hung. Acad.*, 7 (1962), 37–42.
12. P. Erdős and A. Rényi, "Additive properties of random sequences of positive integers", *Acta Arithmetica*, 6 (1960), 83–110; see also "Problems and results in additive number theory", *Coll. theorie des numbres, Bruxelles* (1955), 127–137.
13. P. Erdős, "Density of some sequences of integers", *Bull. American Math. Soc.*, 64 (1948), 685–692.

Nemetvolgyi ut 72^c,
Budapest XII,
Hungary.

Printed by C. F. Hodgson & Son, Ltd., Pakenham Street, London, W.C.1